L. J. Institute of Engineering & Technology
S.G. Highway, Ahmedabad-382210
I.T. / I.C.T Department

Subject Name:	Information and Network Security
Subject Code:	2170709
Branch & Semester:	**IT Sem-VII**

IMPORTANT QUESTIONS

1	Define Cryptography and Cryptanalysis. Draw and explain conventional cryptosystem.
2	Explain the various types of cryptanalytic attack, based on the amount of information known to the cryptanalyst.
3	Explain Play fair Cipher in detail. Find out cipher text for the following given plain text and key. Key = GOVERNMENT Plain text = PLAYFAIR
4	Encrypt the message "Good morning" using the Hill Cipher with the key. 9 4 5 7
5	What is the difference between passive and active security threats? List and briefly define categories of passive and active security attacks.
6	Explain single round function of DES with suitable diagram.
7	Explain DES algorithm with its limitations.
8	Draw and explain Feistel's structure for encryption and decryption.
9	What is the purpose of S-boxes in DES? Explain the avalanche effect.
10	Explain working of AES.
11	Explain Double DES. And Meet-in-the-Middle Attack in detail.
12	List and explain various block cipher modes of operation with the help of diagram.
13	Explain Triple DES in detail.
14	What do you mean by Public key Cryptography? List the Application of Public-Key Cryptosystem. Compare public key and private key cryptography. Also list various algorithms for each.
15	Explain RSA algorithm. P and Q are two prime numbers. P=7, and Q=17. Take public key E=5. If plain text value is 6, then what will be cipher text value according to RSA algorithm? Explain in detail.
16	Write Diffie Hellman key exchange algorithm. Explain man-in-the middle attack on this Diffie Hellman key exchange.
17	Calculate the shared secret (KA and KB) key using Diffie Hellman Key Exchange Algorithm. Take q=23, $\alpha = 5$, XA = 6 and XB = 15
18	Write requirements for hash function and briefly explain simple hash function
19	What is message authentication code? What are the requirements for MACs?
20	Explain HMAC algorithm.
21	Write the Digital Signature Algorithm.
22	What is KDC? With the help of diagram explain how KDC do key distribution.
23	Explain various general categories of schemes for the distribution of public keys.
24	Explain X.509 authentication service
25	Explain Kerberos Authentication System
26	Explain SSL protocol in detail.
27	Explain HTTPS and SSH

28	Write a short note on public key infrastructure
29	What characteristics are needed in a secure hash function?
30	Explain any one approach to Digital Signatures